Exhibit 2

Tech Note

Accu-Time Systems, Inc. 420 Somers Road Ellington, CT 06029 USA
www.accu-time.com Phone: 860-870-5000 Toll Free: 1-800-355-4648 Fax: 860-872-1511

ATS Biometric Devices

This Tech Note provides a description of the available ATS biometric devices (fingerprint readers). In addition it provides answers to many frequently-asked-questions (FAQs). Accu-Time Systems offers three types of biometric fingerscan readers:

- E-Field reader - E-Field readers send a radio wave through the finger to measure the ridges and valleys of the sub-dermal live skin layer. This technology is desirable for environments where fingerprint “spoofing” is a concern.
- Capacitive reader - Capacitive readers use a system of amplifiers to measure the ridges and valleys of the skin as opposed to air. This technology is desirable for high-resolution/low-cost imaging in normal environments.
- Multi-Spectral Imaging reader - The Multi-Spectral reader uses different wavelengths to capture multiple authentication images of structures beneath the skin (blood vessels and oxygenated hemoglobin, collagen, etc). This technology is desirable for difficult environmental conditions where fingerprints are subject to moisture, dirt, dry/arid conditions, as well as genetic or physiological challenges. In addition, it defeats spoofing by measuring the subcutaneous structures in the finger.

Contents

This Tech Note contains the following topics:

Why Use Biometrics? ... 2
User Confidentiality ... 2
Reliability Rules ... 2
ATS Biometric Operational Options ... 3
ATS Biometric Operational Options ... 3
Verification and Identification Modes ... 4
Verification Mode ... 4
Identification Mode ... 4
How it Works ... 5
Recommended Fingers ... 6
Fingerprint Scanner Types ... 7
Image Creation ... 7
Finger Placement ... 11
Frequently Asked Questions (FAQs) ... 14
System Design, Components and Parameters ... 14
Enrollment Process ... 15
Authentication Process ... 17
Fingerprint Templates ... 18
Storage and Security ... 18
Data Retention Policy ... 20

Why Use Biometrics?

Biometric identification provides several advantages over traditional methods that require ID cards/tokens or Password/PIN numbers. Some of the advantages biometric devices provide are:

- Eliminates buddy punching - the person must be physically present at the point-of-identification.
- Provides the ability to eliminate badges/tokens/PINs - identification based on biometric techniques alleviates the need for users to remember a password or carry a token.
- Improves security - protects sensitive and personal data by replacing PINs, eliminates credentials that can be stolen, and prevents unauthorized access to systems or facilities.

User Confidentiality

ATS offers fingerscan biometric devices. Fingerscans are not fingerprints. Many people refer to fingerscans as “fingerprints,” but the data of a fingerscan template is not suitable for law enforcement fingerprint matching. In addition, the reader does not create or save the type of image file required by the Integrated Automated Fingerprint Identification System (IAFIS). The IAFIS is the national fingerprint and criminal history system maintained by the Federal Bureau of Investigation (FBI), Criminal Justice Information Services division (CJIS).

The ATS fingerscan products produce a template that represents points along the unique features and minutia found in a fingerprint pattern. The template files cannot be reverse-engineered to reproduce a fingerprint because the reader does not save the necessary information.

Reliability Rules

Successful biometric installation and use typically requires:

- Management Support (commitment to a maintenance schedule, etc)
- Training of Supervisors and Employees
- Satisfactory Environmental Conditions

Even if all these requirements are met it’s important to note:

- Not all users can be enrolled (for various physiological reasons).
- Biometric devices are susceptible to vandalism.
- Environmental conditions can affect operation (e.g., moisture, dust, cold).

ATS uses these fingerscan technologies for their proven reliability given a few simple rules:

1. All terminals within a facility are installed correctly (installation height observed, obstructions avoided).
2. The employee enrollment procedure is closely followed.
3. The sensor is maintained on a scheduled basis.

ATS Biometric Operational Options

Users may enroll on any terminal and templates can be stored on the scanning terminal or on a host. Templates stored on a host may be distributed to other terminals.

ATS fingerscan readers and terminals provide the following special features:

- Enroll Two Fingers - ATS terminals enable you to configure the fingerscan device to require more than one fingerscan (e.g, index then middle finger).

- Override Verification for Individuals - ATS terminals enable you to disable or set special conditions for certain individuals (in Verification Mode). For example, you can configure the terminal so an amputee can identify/verify without a fingerscan. Alternately, you can configure a user profile to accept any live fingerscan from an individual. This may be necessary if the reader cannot obtain a "good fingerscan" due to physiological issues.

- Adjust False Acceptance Rate - ATS terminals enable you to set the threshold for fingerscan matching accuracy.

Verification and Identification Modes

Verification and Identification Modes are used in time & attendance. During the enrollment process an employee's fingerprint is scanned and converted to a mathematical code, or template. There are no actual "fingerprints" stored anywhere, merely an arithmetic representation of certain minutiae points.

ATS biometric devices have two modes of operation:

- 1:1 Mode (one-to-one mode) or Verification Mode
- 1:N Mode (one-to-many mode) or Identification Mode

NOTE: 1:1 and 1:N templates are not transferable between modes on E-Field readers. The E-Field readers come in either 1:1 Mode or 1:N Mode. You can send templates between E-Field readers but the template only works in the original mode (1:1 or 1:N).

Verification Mode

1:1 Mode is also called Verification Mode. It confirms or denies a person's claimed identity. In this mode the user identifies him or herself using an ID card/token or by entering a password (PIN) at the terminal. Then the person uses the biometric reader to confirm their identity. This process is quick since the terminal/reader recalls the template for the claimed identity and compares it to the current scan.

When an employee presents their identity card or badge at a terminal the reader retrieves that person's fingerscan template. The terminal then prompts the employee to place their finger on the sensor. The reader compares that person's fingerprint to the template held on file and called up by the badge. If the fingerprint being presented matches the one on file for that employee then the match is accepted (good). This is called Verification Mode. It answers the question "Am I the person I say I am?"

Identification Mode

1:N Mode is also called Identification Mode. This method confirms a person's identity by comparing the current fingerscan against a number of enrolled templates (N). This method eliminates the need for ID cards/tokens or passwords/PINs but takes longer to confirm/deny the fingerscan as the number of enrolled templates (N) increases. In addition, a 1:N template is larger than a 1:1 template (file size).

In Identification Mode the employee simply approaches the terminal, presents their finger for scanning, and the entire template database is searched for a matching template. Identification Mode answers the question "Who am I?" This process is simple for the employee and relies on the human body, specifically the fingerprint, as the credential. The company does not need to issue credentials (badges, swipe cards, barcode cards, RFID cards), the employee does not need to carry a card, and the back office infrastructure is less complicated. However, Identification Mode can be a slow process if the template database is large; a problem for enterprises with several hundred or several thousand employees. In large companies Verification Mode may take less than 2 seconds while Identification Mode may take 8 seconds. Multiply 8 seconds by thousands of employees lined up waiting to "punch in" and many hours are wasted.

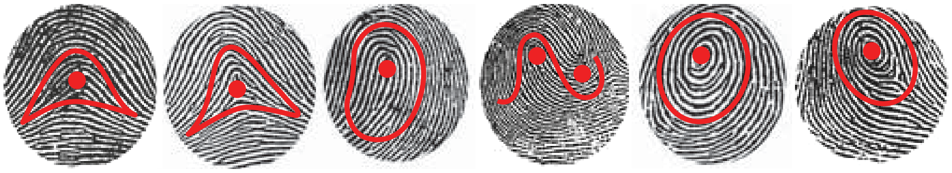
How it Works

At enrollment, the biometric reader scans the user's fingerprint and creates a numeric data template from the fingerprint image. Once it creates the template it discards the fingerprint image/scan. Templates are used for comparison to live fingerscans and are either stored at the terminal or on a host. Templates stored on a host can be distributed to additional terminals.

When a person places his or her finger on the sensor the reader captures an image of the fingerprint. From this point the reader finds unique patterns within the fingerprint. The starting point of this is the fingerprint core. A fingerprint core is a point located within the inner most re-curving ridge. Normally it is located in the middle of the fingerprint as shown in Figure-1.

Figure-1

Location of Fingerprint Core



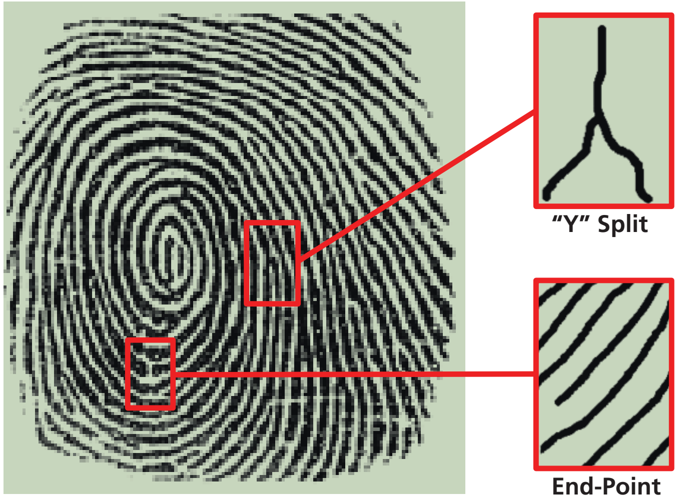
Most frequent types of cores are:

- Arches (plain and tented)
- Loops (singular and twinned)
- Whorl and Central Pocket Loop

The reader also looks for points within the image such as a "Y" split or an end-point as shown in Figure-2.

Figure-2

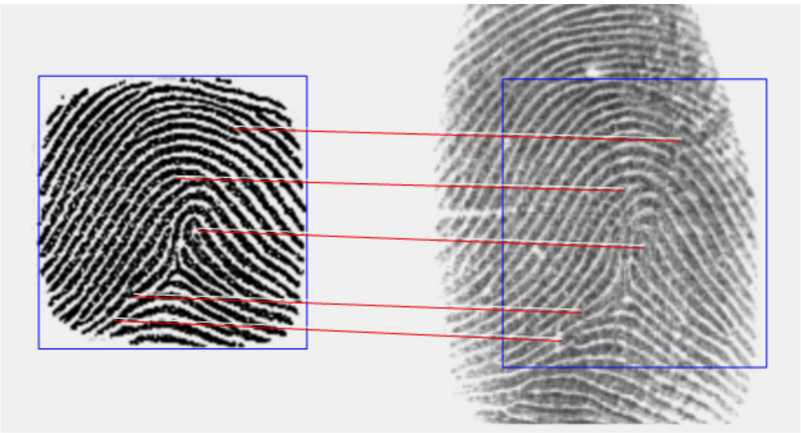
Identifying Points Within Image



Most biometric units only look at the skin surface. These readers are more susceptible to misreads caused by damage on the top layer of the skin. Furthermore, if only the surface layer of skin is examined, the readers can also fall prey to gelatin duplicates of fingerprints.

Figure-3 shows a comparison of an image from a common optical sensor and an image obtained from either a Capacitive or E-Field sensor.

Figure-3 Sensor Comparison



E-Field or Capacitive Sensor

Common Optical Sensor

Recommended Fingers

We recommend users enroll their index, middle or ring fingers. Avoid using the thumb and pinky finger since they are difficult to position on the sensor consistently.

Fingerprint Scanner Types

Accu-Time Systems uses one of three types of fingerprint scanning technologies:

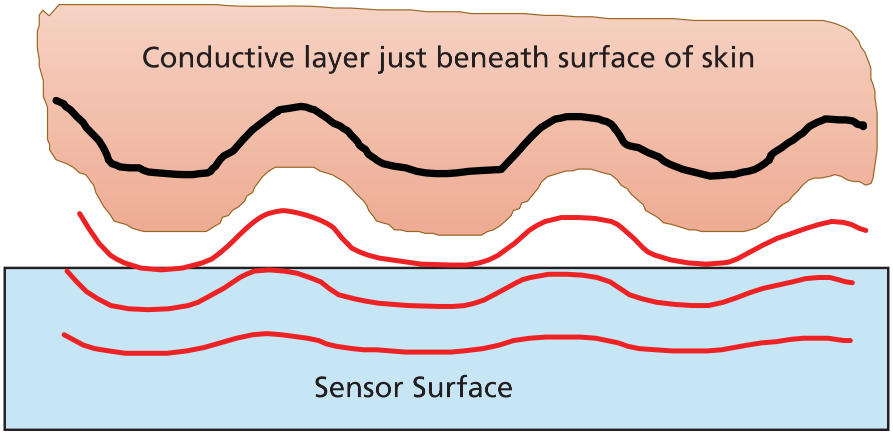
- E-Field Technology (Bioscrypt) - E-Field sensors send a radio wave through the finger to measure the ridges and valleys of the sub-dermal live skin layer.
- Capacitive Technology (Cogent, Suprema) - Capacitive sensors use a system of amplifiers to measure the ridges and valleys of the sub-dermal live skin layer. During enrollment the capacitive reader takes three images of the user's fingerprint and converts all three into a single stored template. Thereafter, the reader verifies the user's subsequent fingerscans using the template.
- Multi-Spectral Imaging Technology (Lumidigm) - The multi-spectral reader uses different light wavelengths (430, 530, 630 nm, and "white light") to capture multiple authentication images of the topical fingerprint and structures beneath the skin.

Image Creation

In general, the sensor detects the ridges and the valleys on the fingerprint as shown in Figure-4. The reader then uses the image to create a numerical fingerscan template or to compare against a template on file. The reader then deletes the scanned image.

Figure-4

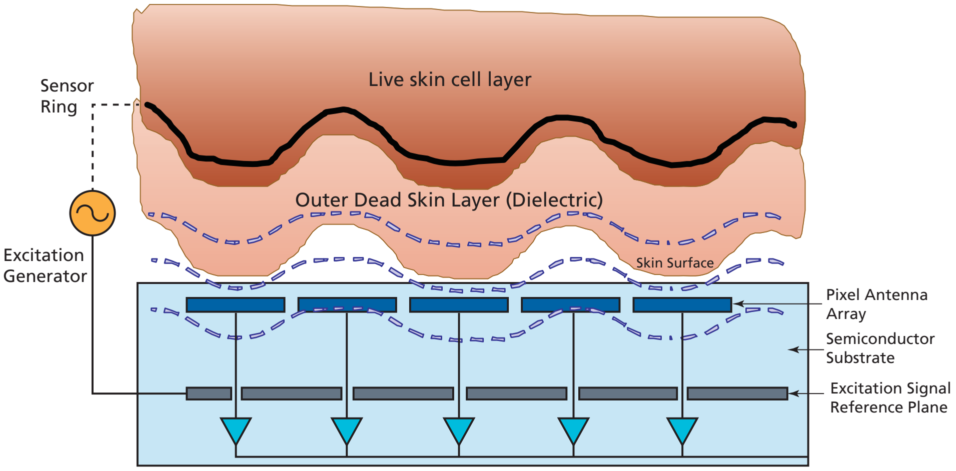
Sensor Detecting Fingerprint Ridges & Valleys



E-Field Sensor

Figure-5 illustrates how an E-Field sensor operates to create a fingerprint image. It shows a cross-section of an E-Field sensor array reading the skin layers of a finger.

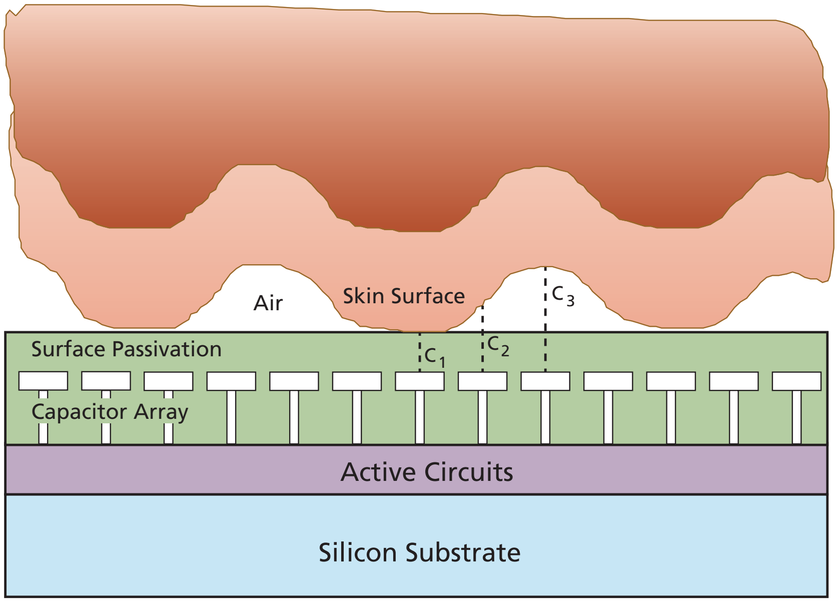
Figure-5 E-Field Sensor Image Creation



Capacitive Sensor

Capacitive sensors use active capacitive pixel-sensing technology to detect the finger ridge and valley patterns. They measure the capacitance of the finger to obtain an image. The capacitance of the finger changes as the distance between the finger and the array changes, C1, C2 and C3, as show in Figure-6.

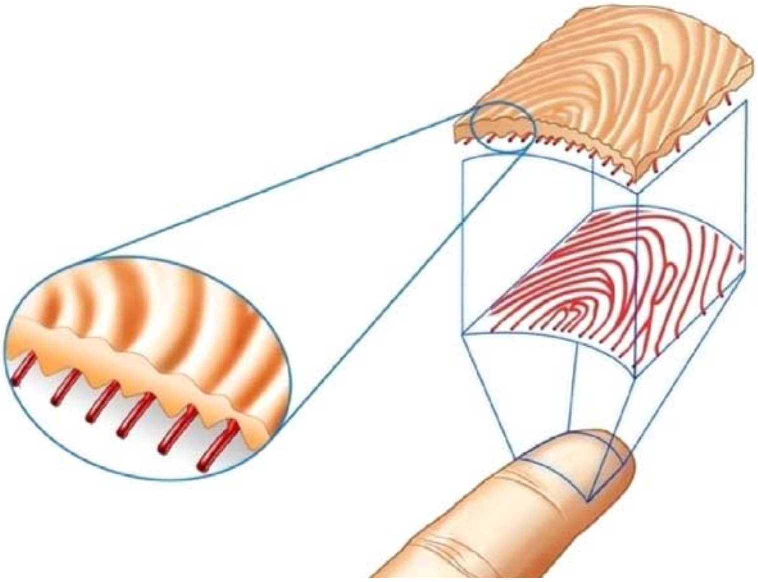
Figure-6 Capacitive Sensor Image Creation



Multi-Spectral Imaging Sensor

The AccuTouch reader uses multi-spectral imaging to authenticate fingerscans. The multispectral sensor has the ability to "see" structures beneath the skin surface (subcutaneous structures). Your "internal fingerprint" is identical to your external fingerprint as illustrated in Figure-7.

Figure-7 Internal and External Fingerprint (Source: Lumidigm Corporation)



The blood vessels and other skin structures are easily imaged with the multispectral approach. Figure-8 shows how oxygenated hemoglobin in blood affects absorption depending on the wavelength of light.

Figure-8 Optical Absorption Due to Blood (Source: Lumidigm Corporation)

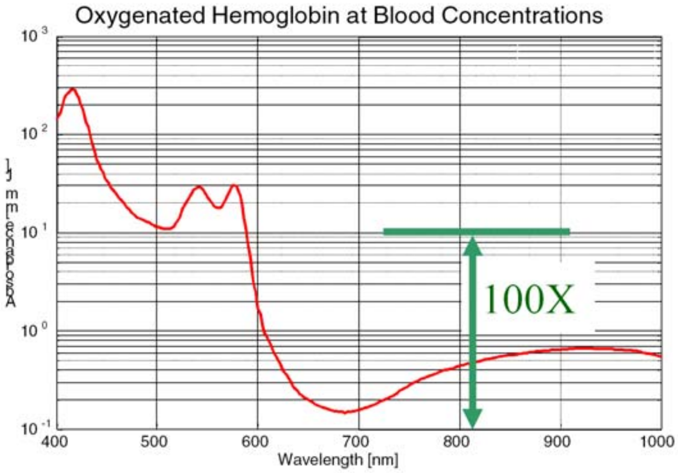
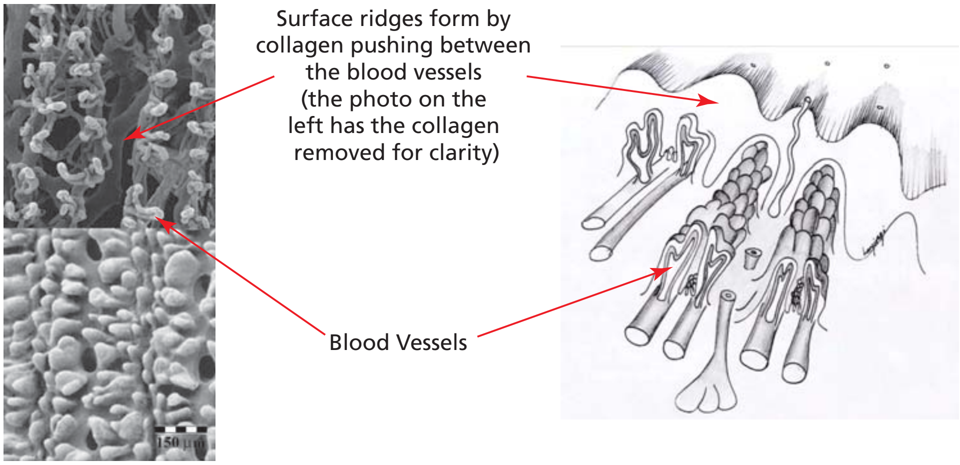


Figure-9 shows how collagen pushing between blood vessels creates ridges in the finger tip.

Figure-9 Relevant Fingertip Physiology (Simone Sangiogi 2006, Source: Lumidigm Corporation)



Surface ridges form by collagen pushing between the blood vessels (the photo on the left has the collagen removed for clarity)

Blood Vessels

Multi-spectral optical fingerprinting using multiple, different images taken on a single reader during a single finger placement offers the following advantages:

- Multiple authentication images at enrollment and during authentication
- Multiple scanning wavelengths
- Different optical geometries
- Surface and subsurface feature identification
- Surface penetration up to 1500 microns deep (1.5 mm)
- “Single reader, single finger placement” for authentication
- No extra user actions

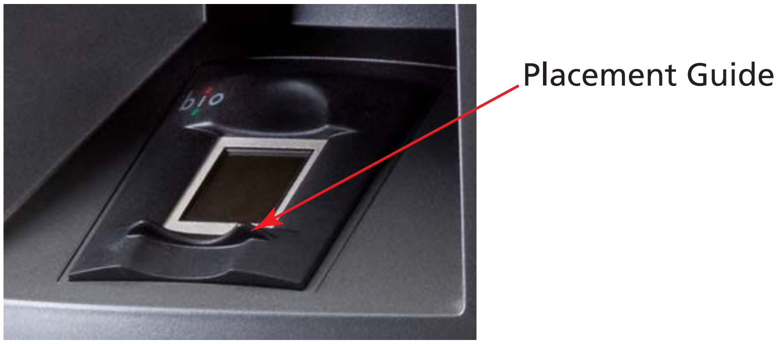
Finger Placement

Filling the sensor area with the fingerprint provides the best performance. Touching the sensor with a fingertip, as if pressing a button, creates scan that lacks information-rich fingerprint data resulting in a rejected authentication.

The placement guide is a raised area located in front of the sensor to aid in finger positioning. Users should center the bottom of their first joint on the placement guide before lowering their finger onto the sensor. Figure-10 shows the placement guide in front of the sensor.

Figure-10

Placement Guide in Front of Sensor



When the terminal displays a message such as "Place finger on reader" or "Present Finger", slide your finger across the placement guide without touching the sensor until the first joint is centered on the placement guide. Use the following procedure to authenticate your fingerprint:

- Align: Position the finger where the center of the first joint meets the center of the placement guide as shown in Figure-11.
- Drop: Lower the finger evenly onto the sensor using moderate pressure as shown in Figure-12.
- Hold: Keep the finger on the sensor until the display shows the acceptance/ rejection message (e.g., "Your finger has been accepted").

Figure-11 Finger Aligned on Placement Guide

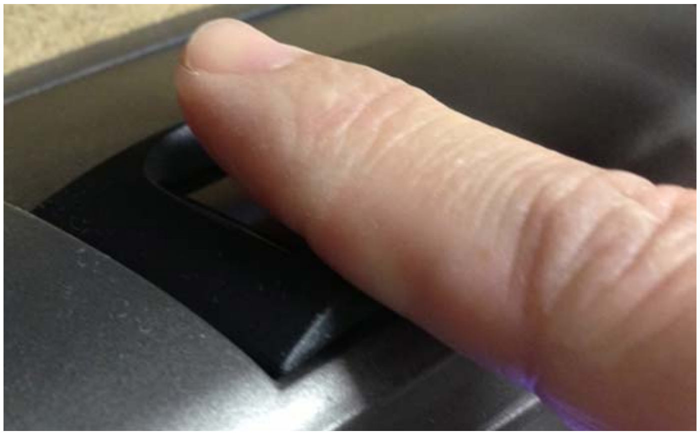
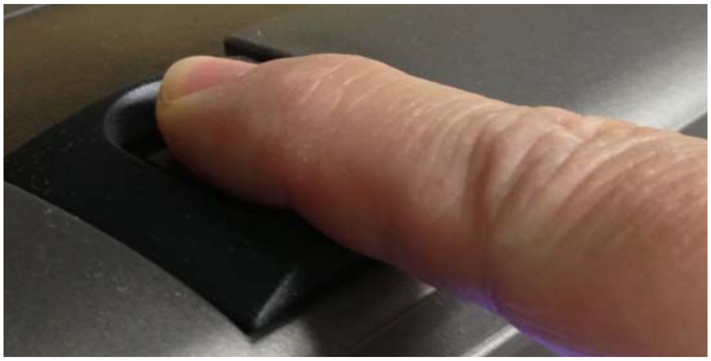


Figure-12 Finger Dropped and Held on Sensor

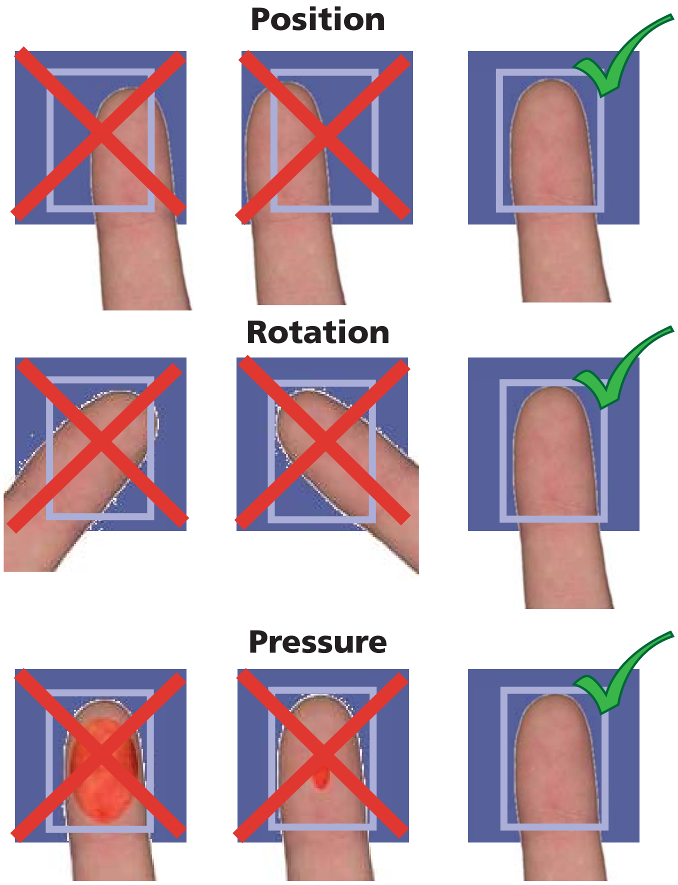


Common issues that produce a rejected authentication are:

- Position: Placing your finger far from the center position of the sensor will increase the rejection rate.
- Rotation: Finger rotation should be kept to a minimum during enrollment and verification.
- Pressure: Apply moderate pressure when making contact with the sensor. Too much pressure may cause smudging of the fingerprint. Too little pressure may not allow the sensor to recognize the presence of a finger.

Figure-13 shows correct and incorrect finger placements.

Figure-13 Correct and Incorrect Finger Placements



Frequently Asked Questions (FAQs)

This sections lists frequently asked questions and provides answers to them. Please contact ATS for questions that do not appear in this section.

System Design, Components and Parameters

This subsection answers common questions about the ATS biometric system design, components, and parameters.

1. *What biometric options does ATS offer?*

   ATS offers three biometric reader options: E-Field, Capacitive, Multi-Spectral. The main differences between these readers include template size, storage capacity, and enrollment procedure.

2. *What are the response times of the biometric options?*

   For Global Series terminals:

   - The E-Field reader in 1:N Mode can scan 150 templates in under one second.
   - The Capacitive reader can scan 500 templates per second. So, if you have 1000 templates in the Capacitive reader, you can expect an average response time of about two seconds. However, if you have 500 or fewer, the average response time is less than a second.
   - The Multi-Spectral reader (template managed/processed by the device):
     Finger placement to image 1.3 sec. (typical)
     Finger placement to template / score 1.8 sec. (typical)
     Finger placement to identification 2.0 sec (typical) - 1,000 users
   - The optional USB-only Multi-Spectral reader (Part Number 98-9013-00) with the template managed/processed by the host PC:
     Finger placement to image 350 ms (typical)
     Finger placement to template / score 400-600 ms (typical)
     Finger placement to identification 500-700 ms - 1,000 users

3. *What are the template sizes?*

   A template is the electronic data that defines the minutiae of a single fingerprint.

   - E-Field readers come in two versions (1:1 and 1:N). The E-Field 1:1 reader template is 384 bytes. The E-Field 1:N reader template is 2352 bytes.
   - The Capacitive reader uses a single 784 byte template for both 1:1 and 1:N matching.
   - The Multi-Spectral reader template is 1592 bytes.

4. *Is enrollment and authentication done locally or on a server?*

   Enrollment occurs locally and can be forwarded to the host. No image is stored.

5. *Which hardware and software products from the vendor are used? Can you provide specifications for those products?*

   ATS doesn’t provide any additional specifications. For additional information and specifications see the following websites:
   http://www.cogentsystems.com
   http://www.supremainc.com/eng/main.php
   http://www.bioscrypt.com
   http://www.lumidigm.com

   Contact ATS for the model and vendor of your reader.

6. *In the case of a one-to-many identification system, how many templates is the system capable of matching (e.g., 1:3000, 1:20000)?*

   For Global Series terminals:

   - The E-Field 1:N reader can store up to 200 templates. (The E-Field 1:1 reader can store up to 4,000 templates.)
   - The Capacitive reader with 8 MB storage can store up to 9,000 templates.
   - The Multi-Spectral reader can store up to1000 templates in Identification (1:N) mode

7. *Does the system create a record of attendance, transactions, or both? How are those data used?*

   A transaction is recorded with a date and time stamp. It is used for diagnostics as needed. See the ATS Universal Command Set (UCS) Reference Manual for information about data and badge number formats.

8. *What is the durability of the biometric readers?*

   The readers meet the following ESD immunity certifications:

   - The Capacitive readers are certified to IEC 610000-4-2 level 4 (+/- 15KV)
   - The E-Field readers are certified to IEC 610000-4- 2 level 3 (+/- 8KV)
   - The Multi-Spectral reader is certified to IEC 61000-4-2 Level 4 (+/-15 kV Air)

Enrollment Process

This subsection answers common questions regarding the enrollment process.

1. *How does enrollment differ for the E-Field, Capacitive, and Multi-Spectral readers?*

   - The E-Field reader enrollment process is more interactive, using a three-tiered approach for quality and content of the fingerprint. It returns enrollment quality and content scores, which a user’s application can evaluate to determine if the enrollment is adequate for acceptance.
   - The Capacitive reader enrollment process is more automated. The reader evaluates the fingerscans taken for enrollment and takes multiple scans as necessary until reliable scans are obtained.

- The Multi-Spectral reader requires three separate finger placements and scans at enrollment. It then uses the best scan to create the template.

2. *How many and which fingers (e.g., right index plus left index) are needed for each enrolled user (enrollee)?*

   The number of fingers enrolled is controlled by your system integrator or administrator, but ATS recommends the enrollment of two fingers. The recommended enrollment fingers are the index finger on the right and left hands. We do not recommend enrolling the thumb or pinky finger.

3. *How many fingers and which ones are normally needed for authentication (i.e., one of the enrolled fingers or both)?*

   In 1:1 Mode, one of the enrolled fingers is required.

4. *Is submission of fingerprints voluntary for a user? What are the other options available to the user?*

   In 1:1 Mode, ATS terminals provide an option to not use the fingerscan device. ATS terminals enable you to disable or set special conditions for certain individuals. For example, you can configure the terminal so an amputee can identify/verify without a fingerscan. Alternately you can configure a user profile to accept any live fingerscan from an individual. This may be necessary if the reader cannot obtain a “good fingerscan” due to physiological issues.

5. *Does dry skin affect the readers?*

   If there is excessive dryness to the finger it is possible that the E-Field or Capacitive reader may have difficulty achieving an adequate scan. In case of this rare event, some customers have installed a moisturizing agent next to the terminal.

   The Multi-Spectral reader can detect and identify a fingerscan regardless of dryness that can result from cold, location (high desert), activity (flying), health, diet, or natural skin characteristics.

6. *Some users do not have fingerprints of acceptable quality and there is a failure to enroll. How are these cases handled?*

   For the E-Field reader, there are multiple verification levels available to accommodate different quality levels. Enrollees can be placed into an exception list allowing them to pass with little or no verification.

   The Capacitive reader has three levels of verification: “verify”, “verify-anything”, or “don’t ask for enrollment”. In 1:N Mode, there are no adjustments that help the employee to enroll.

   The Multi-Spectral reader can detect and identify a fingerscan regardless of factors such as soft fingerprint ridges dues to aging, dry fingertips (as described previously), wet or dirty fingerprints, or conditions of high ambient light that oversaturates conventional readers.

7. *Can 100% enrollment success be guaranteed?*

   While there are constant improvements in biometric technologies such as fingerscan readers, there will always be a very small percentage of the population who cannot be read for one reason or another.

8. *During enrollment, is there a way for anyone, such as an employee, to capture the image using the Print Screen button?*

   No image is ever displayed on a screen, therefore images cannot be viewed or captured using the Print Screen button or other function.

Authentication Process

This subsection answers common questions regarding the authentication process.

1. *Is authentication done under supervision or in the presence of a security guard?*

   Enrollment is typically administered by a supervisor; authentication does not require any supervision.

2. *How is a false rejection handled, especially for users having difficulties with the system?*

   For the E-Field reader, the false rejection rate (FRR) is 0.1% and the false acceptance rate (FAR) is 0.1% for one finger.

   For the Capacitive reader, FRR is 0.1% to 0.001% and the FAR is 0.01% to 0.0001%.

   For the Multi-Spectral reader you can adjust the acceptance/rejection sensitivity in the ATS terminal via the FPVL command in the Universal Command Set with the following values:
   1 = Very High Security
   2 = High Security
   3 = Medium Security (default)
   4 = Low Security
   5 = Very Low Security

   The Multi-Spectral reader FAR/FRR for each setting is:
   1 = 30000, FAR = 0.01%, FRR = 2.5% (Very High Security)
   2 = 27520, FAR = 0.05%, FRR = 1.8% (High Security)
   3 = 26350, FAR = 0.1%, FRR = 1.4% (Medium Security)
   4 = 23540, FAR = 0.5%, FRR = 1.0% (Low Security)
   5 = 22645, FAR = 0.82%, FRR = 0.8% (Very Low Security)

3. *Does the user see the fingerprint image during authentication? (e.g., are there monitors on site to display the image)*

   No image is displayed during authentication.

4. *After the fingerprint authentication, does the system use any other means (e.g., a person's photo), to further confirm their identity?*

   PIN and badge numbers can be used for identity; no other methods, such as photographs, are used.

Fingerprint Templates

This sections answers common questions regarding fingerprint templates.

1. *Are the fingerprint templates compatible, or can they be made compatible, with one of the following standards: ANSI-INCITS 378, ISO/IEC 19794-2, FIPS 201, or ILO SID-0002?*

   No, the template is only recognized by the reader type that created it. There is no other way to extract useful information from the template.

2. *Does the template contain fingerprint minutiae (details of interest in a fingerprint), such as x and y positions and directions?*

   Yes, this information is contained in an ASCII format.

3. *Does the template contain the following data: minutiae type, quality, fingerprint core and delta positions, ridge count, and orientation field?*

   No, the template is a series of ASCII characters and there is no image identifying fingerprint core, ridge count, etc.

4. *Is the template size fixed or variable?*

   The template size is fixed by the type of reader being used.

Storage and Security

This subsection answers common questions regarding storage and security.

1. *Where are the templates stored (e.g., locally or on a server)?*

   Templates are stored on the terminal or on a host. Backup copies of the templates should be stored on the host.

2. *Are the fingerprint images stored on a server or somewhere else in the system? Is storing or not storing the image a configurable option? If so, who does the configuration?*

   No image is available or stored. Readers discard scanned images when they create templates.

3. *Are the stored templates encrypted?*

   Encryption and other security methods are controlled by the system integrator or administrator. Data transferred from the terminal to the host can optionally be set for encryption.

4. *How are the stored data protected (e.g., from an insider's attack or if the server is stolen)?*

   Data protection is controlled by the system integrator or administrator.

5. *Who has access to the stored templates? How is access controlled?*

   Template access is controlled by the system integrator or administrator.

6. *Does the biometric vendor regularly access the stored templates?*

   Templates are stored on the terminal and can be accessed by the system integrator or administrator in some situations. The manufacturer of the biometric reader does not have direct access to data stored on any ATS device.

7. *How are the upgrades and maintenance of the biometric system performed?*

   Upgrade and maintenance is at the discretion of the system integrator or administrator.

8. *How and where is the template storage backed up?*

   Backup options are available from and controlled by the system integrator or administrator.

9. *Is a wireless connection used anywhere in the system? If so, is it encrypted?*

   Partners have the option to add a wireless modem to the terminal with either standard or enterprise encryption.

10. *Are the biometric servers connected to the Internet or an intranet?*

    The terminal can be installed in Internet mode at the discretion of the system integrator or administrator.

11. *What are the safeguards, if any, against spoofing (e.g.,applying a fake fingerprint)?*

    The readers use different technologies to prevent fingerprint spoofing. Some of these technologies are:

    - using an advanced analysis algorithm to detect the abnormalities in dynamic changing patterns of fingerprint images.
    - measuring the optical characteristics of the skin below the surface enabling a strong discrimination between living human skin and spoofs.

      Please contact ATS to determine which reader technology best meets your security environment and requirements.

12. *If there is a request from a law enforcement agency, can the biometric template be extracted from the system? What is the procedure? Who will perform the extraction?*

    No, since the template is not a fingerprint image it is useless to law enforcement agencies.

13. *What are the environmental requirements of the readers?*

    The E-Field reader is rated for 0 to 60°C (32 to 140°F).

    The Capacitive reader is rated for 0 to 55°C (32 to 131°F). If operated within these temperature ranges, the performance (read rate) of each reader is independent of ambient temperature.

    The Multi-Spectral reader is rated for -10 to 60°C (14 to 140°F).

14. *Are biometric readers easy to clean?*

    Both reader options can be easily cleaned using any mild cleaning method. Mild liquid cleaners are appropriate provided that the reader is not exposed to excessive amounts of liquid.

Data Retention Policy

This subsection answers common questions regarding the data retention policy.

1. *How long is the biometric information retained in the system?*

   Information can be retained for the life of the system.

2. *Can users request the deletion of their biometric information?*

   Yes, templates can be erased through a purge-templates command executed by the system integrator or administrator.